ABSTRACT OF THE DISCLOSURE

A method and a system for generating prime numbers and testing for primality of an integer. This invention has applicability to "public key" and other encryption techniques that play an important role in the security of information technology and electronic commerce. Generation of prime numbers requires the step of testing the primality. The method includes a deterministic test for testing the primality of a number in polynomial time. The system comprises a random number generator and a primality tester. The random number generator generates a random number and the primality tester tests the primality of this random number. The primality tester can also be used independent of the random number generator. In such a case, the number whose primality is to be tested can be input via a user interface.